WHAT IS CLAIMED IS:

1. A method for detecting a computer virus in a data stream comprising:

estimating a scan time period required to scan the data stream;

scanning the data stream to detect at least one computer virus if the estimated scan time period does not exceed a maximum scan time period; and

transmitting the data stream without the scanning if the estimated scan time period exceeds the maximum scan time period.

2. A method according to claim 1, wherein the maximum scan time period is predetermined.

3. A method according to claim 1, wherein the maximum scan time period is dynamically determined.

4. A method according to claim 1, further comprising:

activating remedial action upon detecting the at least one computer virus in the data stream.

5. A method according to claim 1, wherein the data stream is included in a streaming data file.

6. A method according to claim 1, wherein the maximum scan time period is one of a plurality of maximum time periods.

7. A method according to claim 4, wherein the remedial action comprises:

logging an event of virus detection.

8. A method according to claim 4, wherein the remedial action further comprises:

stopping a transfer of the data stream if the transfer is still in progress.

9. A method according to claim 4, wherein the remedial action further comprises:

notifying users of the data stream.

10. A method according to claim 4, wherein the remedial action further comprises:

blocking a uniform resource locator corresponding to the data stream.

11. A method according to claim 10, wherein the remedial action further comprises:

advertising the uniform resource locator corresponding to the data stream to one or more network elements in a network.

12. A method according to claim 4, wherein the remedial action further comprises:

blocking one or more uniform resource locators similar to the uniform resource locator corresponding to the data stream.

13. A method according to claim 4, wherein the remedial action further comprises:

initiating virus cleaning actions.

14. A network comprising:

at least one network element configured to

estimate a scan time period required to scan a data stream;

scan the data stream to detect at least one computer virus if the estimated scan time period does not exceed a maximum scan time period; and

transmit the data stream without scanning if the estimated scan time period exceeds the maximum scan time period.

15. A network according to claim 14, wherein the network element is further configured to

activate remedial actions upon detecting the at least one computer virus in the data stream.

16. A network according to claim 14, wherein the maximum scan time period is predetermined.

17. A network according to claim 14, wherein the maximum scan time period is dynamically determined.

18. A network according to claim 14, wherein the data stream is included in a streaming data file.

19. A network according to claim 14, wherein the maximum scan time period is one of a plurality of maximum time periods.

20. A network element comprising:

a processor;

a data receiver coupled to the processor and configured to receive a data stream, wherein the processor is configured to

estimate a scan time period required to scan the data stream;

scan the data stream to detect at least one computer virus if the estimated scan time period does not exceed a maximum scan time period; and

transmit the data stream without scanning if the estimated scan time period exceeds the maximum scan time period.

21. A network element according to claim 20, wherein the maximum scan time period is predetermined.

22. A network element according to claim 20, wherein the maximum scan time period is dynamically determined.

23. A network element according to claim 20, wherein the processor is further configured to

activate remedial actions upon detecting the at least one computer virus in the data stream.

24. A network element according to claim 20, wherein the data stream is included in a streaming data file.

25. A network element according to claim 20, wherein the maximum scan time period is one of a plurality of maximum time periods.

26. A computer program product encoded in one or more computer readable media, the computer program product comprising:

an execution sequence of instructions, the execution sequence of instructions is configured to estimate a scan time period required to scan a data stream;

scan the data stream to detect a computer virus if the estimated scan time period does not exceed a maximum scan time period; and

transmit the data stream without scanning if the estimated scan time period exceeds the maximum scan time period.

27. A computer program product according to claim 26, wherein the execution sequence of instructions is further configured to:

activate remedial actions upon detecting the at least one computer virus in the data stream.

28. A computer program product according to claim 26, wherein the execution sequence of instructions is further configured to:

log an event of virus detection.

29. A computer program product according to claim 26, wherein the execution sequence of instructions is further configured to:

stop a transfer of the data stream if the transfer is still in progress.

30. A computer program product according to claim 26, wherein the execution sequence of instructions is further configured to:

notify users of the data stream.

31. A computer program product according to claim 26, wherein the execution sequence of instructions is further configured to:

block a uniform resource locator corresponding to the data stream.

32. A computer program product according to claim 26, wherein the execution sequence of instructions is further configured to:

advertise the uniform resource locator corresponding to the data stream to one or more network elements in a network.

33. A computer program product according to claim 26, wherein the execution sequence of instructions is further configured to:

block one or more uniform resource locators similar to the uniform resource locator corresponding to the data stream.

34. A computer program product according to claim 26, wherein the execution sequence of instructions is further configured to:

initiate virus cleaning actions.